One time pad

Message XOR Key = Encoded message

- The key with no information itself
- Easy to decode with a key
- Impossible to decode without a key in a mathematical, logical way
- Must share key physically -> impractical

Ex.

Message	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	0
Key	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	1	1	0	1	0	0	0	1	1

Encoded	0	1	0	1	0	1	1	1	1	0	0	1	0	0	1	0	0	0	1	0	0	1	0	1

Public key cryptography – RSA method

Using public key and private key

- Public key: shared with everyone in the world
- Private key: kept individually -> ensure the communication to be secured
- Complicated than a one-time pad

Problems

- Current mathematics may be discovered the way of breaking
- A quantum computer will be able to break this method

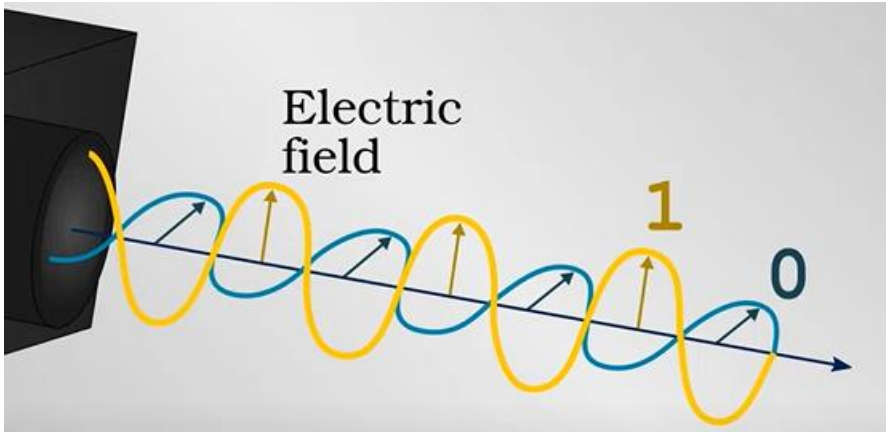
-> Going back to the one-time pad, but more practically with quantum physics

Photon polarisation

Polarisation: oscillating in a specific direction

- A one-time key could be found using this characteristic

Ex. up down: 1 / side to side:0



Security is guaranteed by using polarisation

- the characteristic is a quantum mechanical property -> can be in a superposition of two mutually exclusive outcomes

- oscillating up-and-down and side-to-side simultaneously

- If there is eavesdropping by someone, the superposition would collapse

  -> Communicators notice the presence of ‘someone’

  -> Throw away the key and try again later / call the police

  -> If there is no collapsing, no one knows the key

BB84

Creating a one-time pad between a sender and a receiver

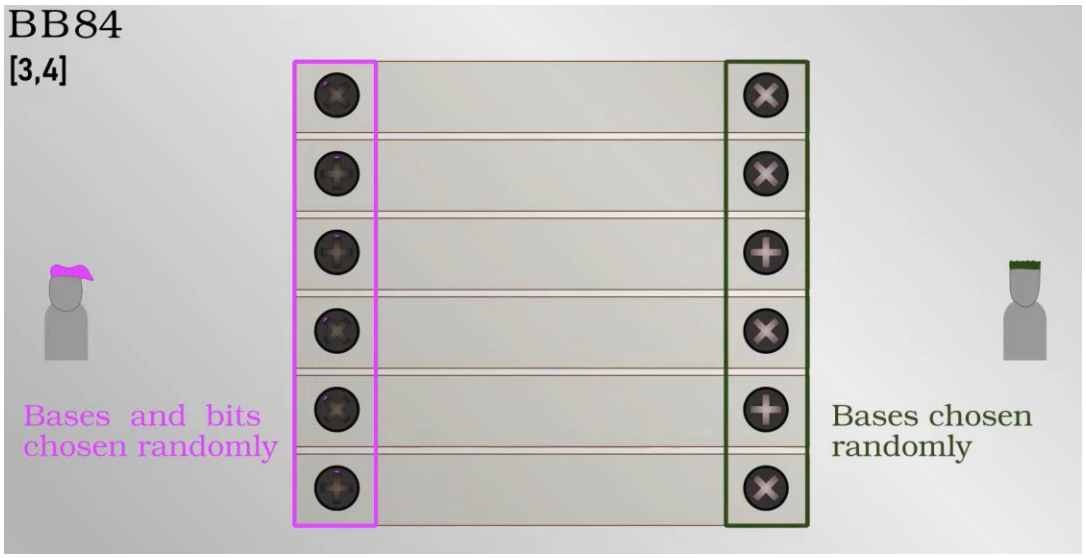
- define two polarisations that represent states of 0 and 1

- measure them on a rectilinear basis and diagonal basis

Ex.

How?

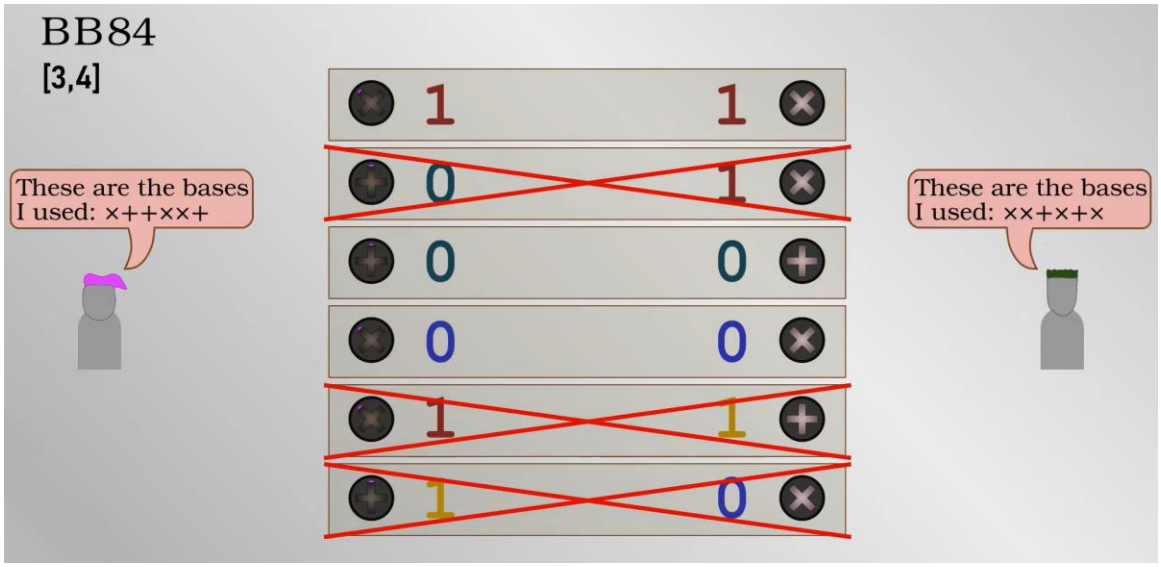
1. A sender chooses basis and bits randomly while a receiver chooses basis



2. The receiver gets the bits sent by the sender through a chosen filter

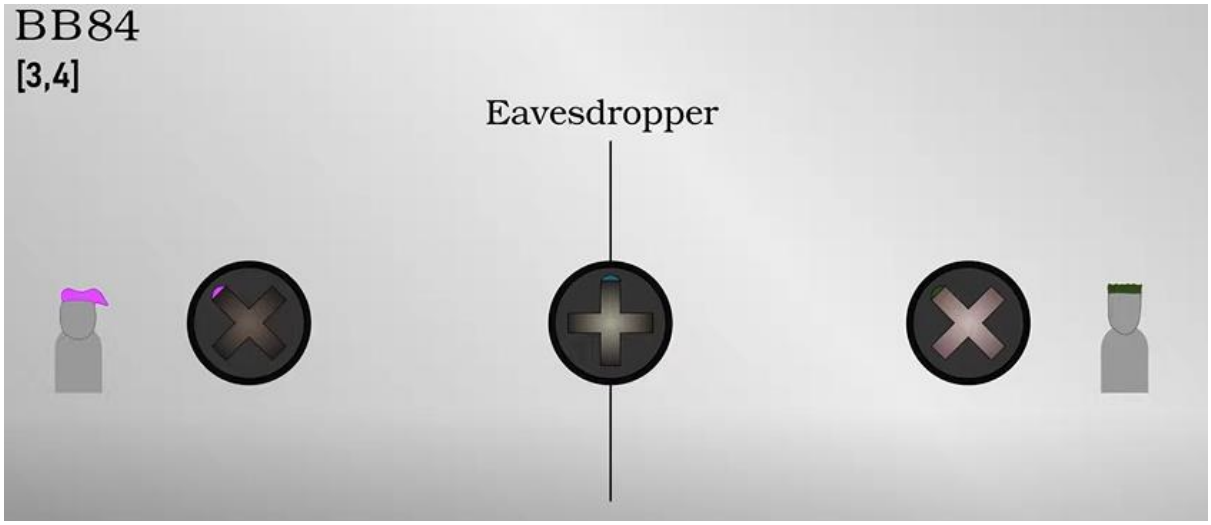
3. Eliminate signals that do not match to avoid incorrect answers -> receiver could get the wrong answer

4. Share basis publicly -> not bits themselves, only basis



5. Use a found one-time-key, in the example, it will be 100

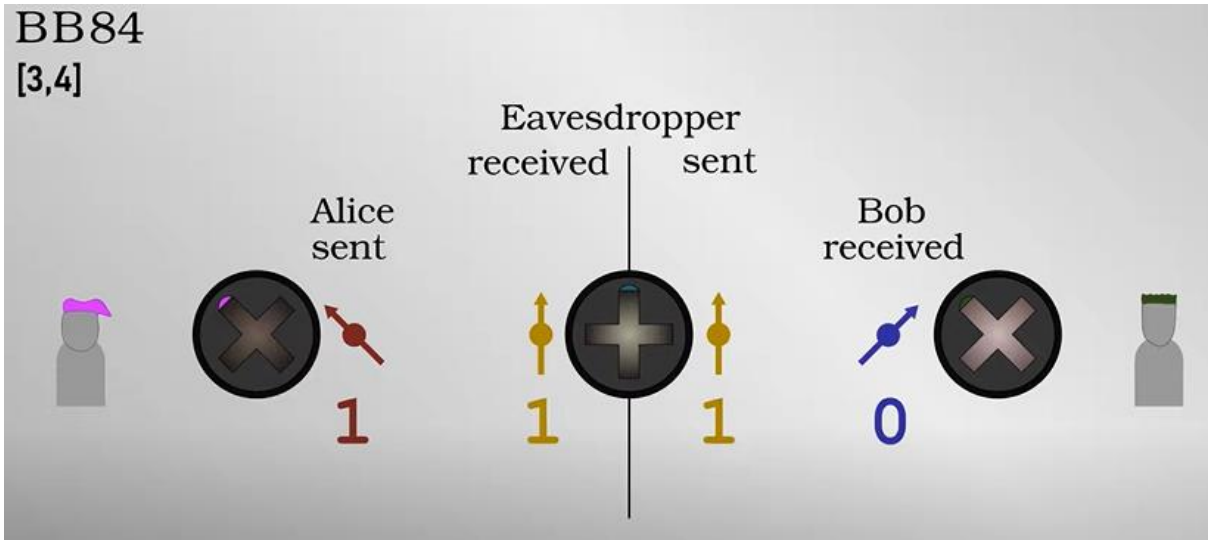
In the case of an eavesdropper?



- Imagine this case, the eavesdropper will measure the sent photons and resend them to the receiver

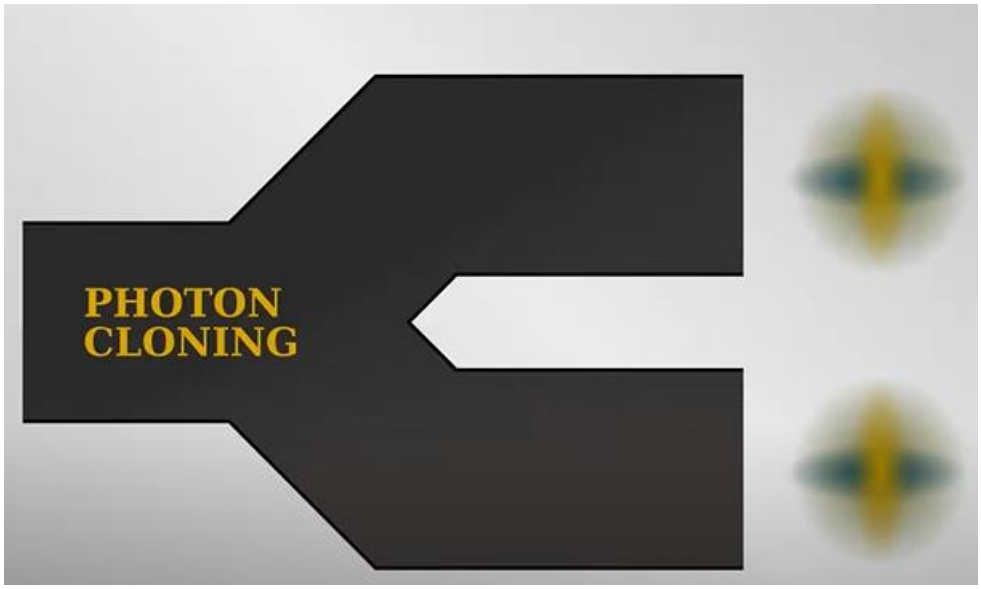
- As the eavesdropper doesn't know which basis was used -> inevitably chooses the wrong one at some point

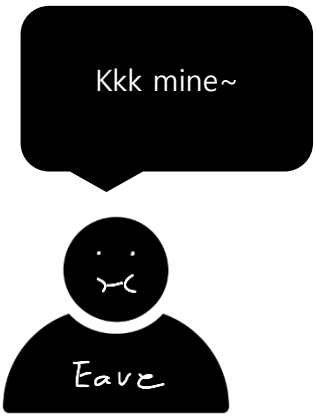
- In addition, communication will be messed up



- By comparing photons publicly, eavesdroppers would be found easily

Photon cloning is strictly prohibited in quantum mechanics: no-cloning theorem





- The theorem indicates that this situation is impossible

- Getting the photon without disturbance could not happen

The BB84 method allows people to make quantum internet

- Satellite also utilizes this, establishing secure connections from the ground.

- Communication through space by fibre optics is possible everywhere on Earth

E91

Creating a one-time pad between a sender and a receiver using entangled pairs of photons

- Different from BB84 because it uses single photons

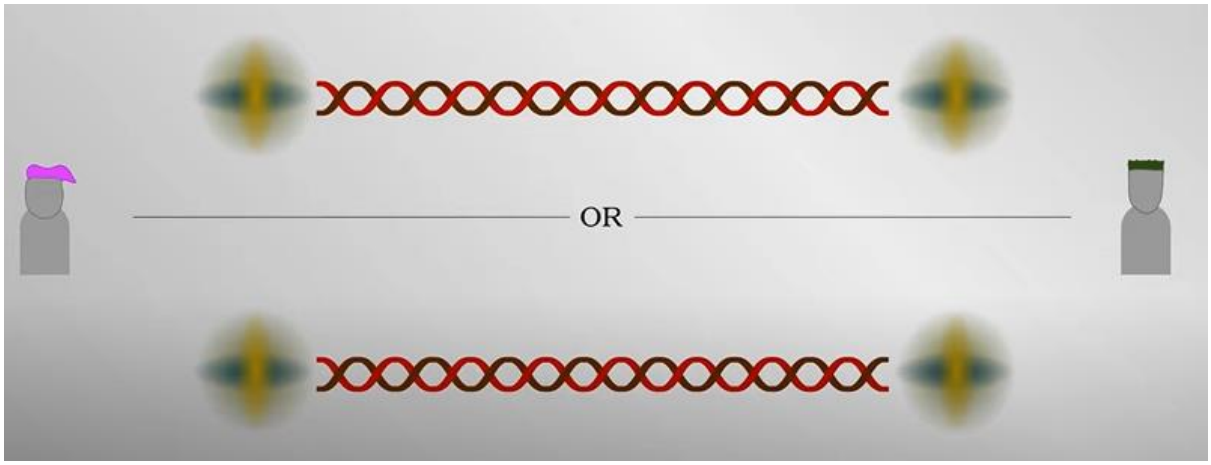
- Entangled states are correlated

Correlation of entangled pairs of photons

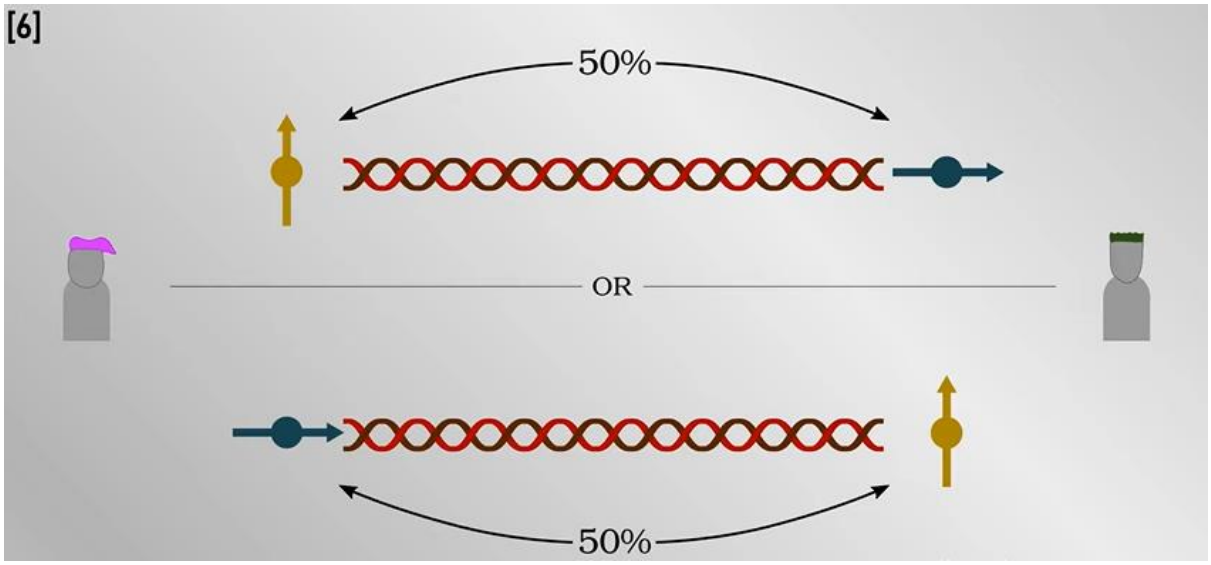
- measuring one affects the other like below

How?

1. A sender and a receiver each get one of a pair of photons, whose name is Bell singlet state



2. A sender will get the result of 0 of 1 in equal probability

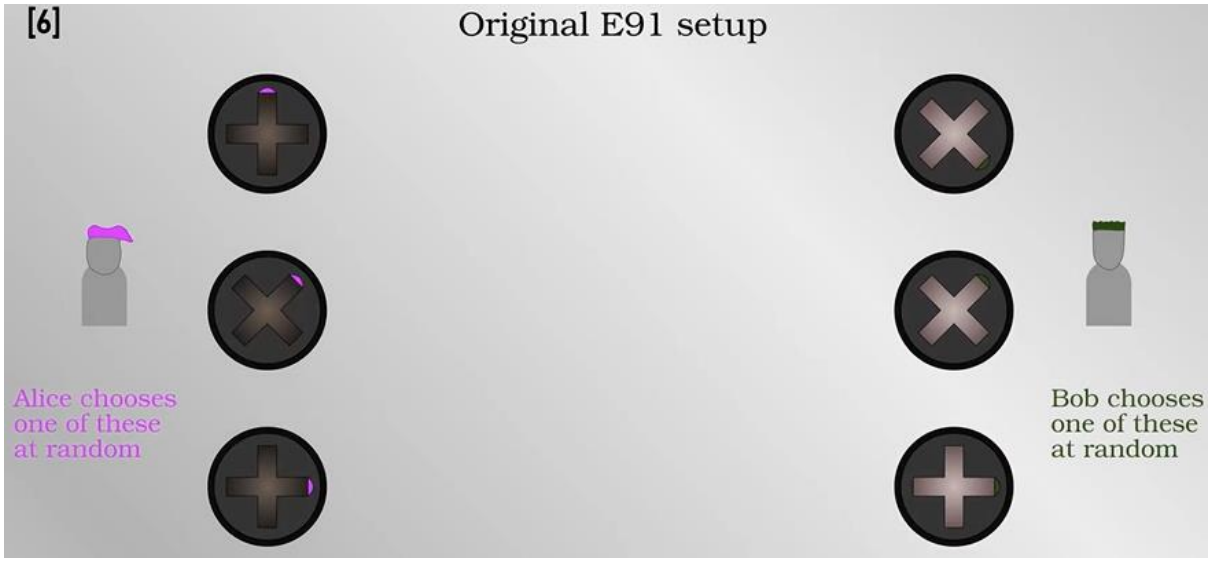


- A receiver must obtain the opposite of what the sender measures as long as the receiver uses the same basis

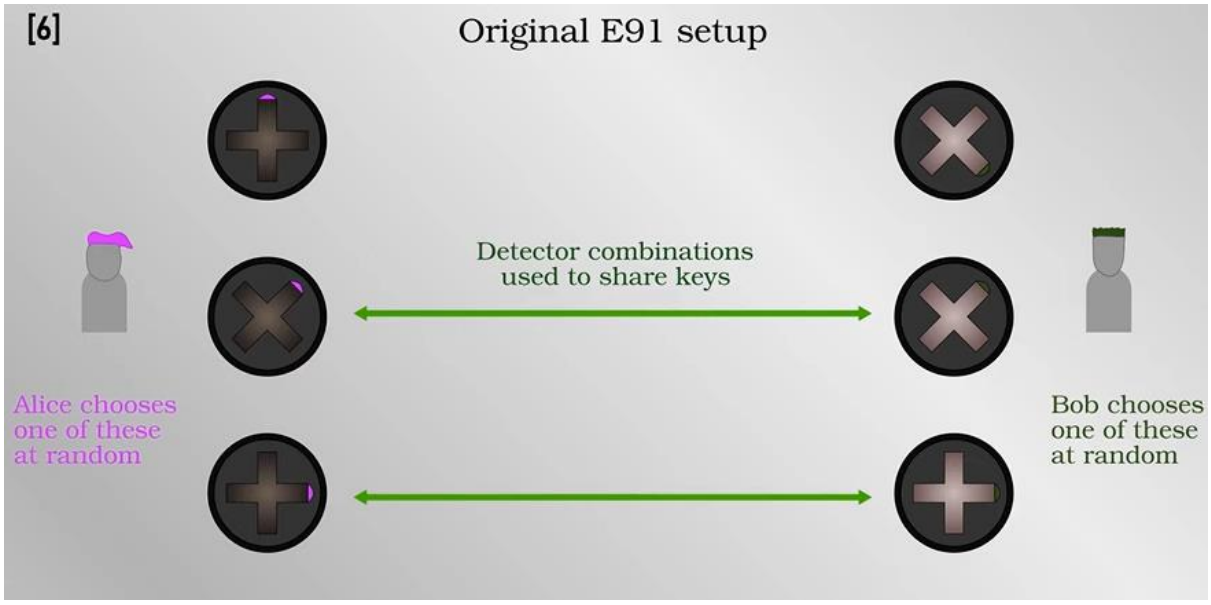
- A measurement that the sender makes influences the photon of the receiver or vice versa

- The outcome of the first measurement cannot be predicted until it is made

3. Choose the basis respectively



4. Share measurement basis and find the time when they used same basis



5. The chosen one will produce a random key because they are entangled

In the case of an eavesdropper?

- If an eavesdropper intercepts the pair, the entangled pair will be destroyed and will no longer be correlated

- The broken correlation can be detected